Privacy-SPS

v.2.5.0.0

ФУНКЦИОНАЛЬНАЯ СПЕЦИФИКАЦИЯ

020314-2.5.0.0-35

2025 г.

Аннотация

Настоящий документ содержит описание функций, назначения, условий использования системы поддержки процессов обработки и защиты ПДн «Privacy-SPS» (далее СПП ПДн).

В процессе использования комплекса решаются следующие задачи:

- учет состава и структуры ИСПДн, процессов обработки и защиты ПДн;
- учет и формирование требований к процессам обработки и защиты ПДн;
- реализация (поддержка реализации) требований к процессам обработки и защиты ПДн;
- контроль соответствия процессов обработки и защиты ПДн нормативным требованиям;
- сигнализация о необходимости внесения изменений в процессы обработки и защиты ПДн.

Содержание

Перечень сокращений

АРМ	Автоматизированное рабочее место
ИСПДн	Информационная система персональных данных
ПДн	Персональные данные
ПО	Программное обеспечение
СЗПДн	Система защиты персональных данных
СКЗИ	Средство криптографической защиты информации
СПП ПДн	Система поддержки процессов обработки и защиты ПДн

1. Введение

1.1. Цели использования

Целью использования программного комплекса является:

- Выполнение требований закона «О персональных данных» в части управления безопасностью процессов обработки ПДн.
- Автоматизация рутинных операций связанных с обработкой и обеспечением безопасности ПДн.
- Организация мониторинга изменений процессов обработки ПДн.

1.2. Состав программного комплекса

Программный комплекс «Privacy-SPS» является **дополнительным модулем** к системе «LIS-SPS».

1.3. Порядок использования

Работа в СПП ПДн осуществляется в следующем общем алгоритме:

1. Ввод данных в СПП ПДн пользователями, либо загрузка данных из внешних систем.
2. Автоматический анализ введенных данных, определение несоответствий в процессах обработки и защиты ПДн.
3. Генерация необходимых документов в автоматизированном режиме, выполнение других действий по приведению процессов в соответствие.
4. Ввод данных об изменениях в процессах, системах – повтор шагов 1-3.

Система позволяет:

- Обеспечить автоматизированный ввод данных о структуре и составе процессов обработки ПДн, ИСПДн, активов из разных подразделений в четко определенном формате.
- Вести работу с субъектами ПДн, генерировать необходимые согласия субъектам ПДн, контролировать сроки отправки документов.
- Обеспечить автоматическую загрузку и анализ данных из внешних источников – кадровых баз данных, систем учета данных по субъектам ПДн, систем инвентаризации технических средств информационных систем, CRM и IDM систем
- Обеспечить автоматизированную генерацию необходимых документов (актов, приказов, журналов учета, описаний и т.п.) по введенным данным.

- Контролировать корректность введенных данных, необходимость обновления выпущенных документов, проверять необходимость уничтожения ПДн.

АРМ оператора, как правило, используется на рабочих местах ответственных:

- в пользовательских структурных подразделениях, участвующих в процессах обработки и защиты ПДн,
- в ИТ подразделениях,
- в подразделениях ответственных за защиту ПДн.

Внедрение программного комплекса предполагает разные сценарии использования. Например, возможен следующий режим работы при выполнении требований в области ПДн:

- На АРМ пользовательских подразделений, в случае изменения процессов обработки ПДн, либо в случае появления новых активов, процессов, носителей ПДн осуществляется ввод учетных данных в СПП ПДн.
- На АРМ ИТ отделов осуществляется ввод данных о составе серверов, сетевого оборудования, баз данных, архитектуре ИСПДн.
- На АРМ ИТ отделов осуществляется генерация документации по ПДн находящейся в области ответственности ИТ, например, журналов учета средств защиты и т.п.
- На АРМ отделов осуществляющих работу с субъектами ПДн, по введенным данным о процессах обработки ПДн, осуществляется генерация согласий, иных необходимых документов и т.п.
- На АРМ отделов ответственных за защиту ПДн, по введенным данным, осуществляется генерация документов в области защиты ПДн, например, Перечня ПДн и т.п.
- На АРМ ответственного за организацию обработки ПДн осуществляется анализ введенных данных, выявление несоответствий, выдача корректирующих действий.

Система поддержки процессов защиты и обработки персональных данных «Privacy-SPS» имеет следующие основные показатели:

- включает более 100 функций по контролю процессов обработки и защиты ПДн, вводу данных и генерации документов,
- позволяет произвести порядка 20 видов проверок процессов на соответствие требованиям в области ПДн.

2. Описание комплекса

2.1. Функции комплекса

СПП ПДн обеспечивает реализацию следующих дополнительных[1] функций:

1. Управление процессами обработки ПДн, включая:

1.1. учет технологических процессов обработки ПДн, включая процессы взаимодействия с контрагентами, а также иерархии процессов,

1.2. учет нормативных, договорных и других оснований для обработки ПДн, необходимости получения согласий субъектов ПДн по каждому основанию,

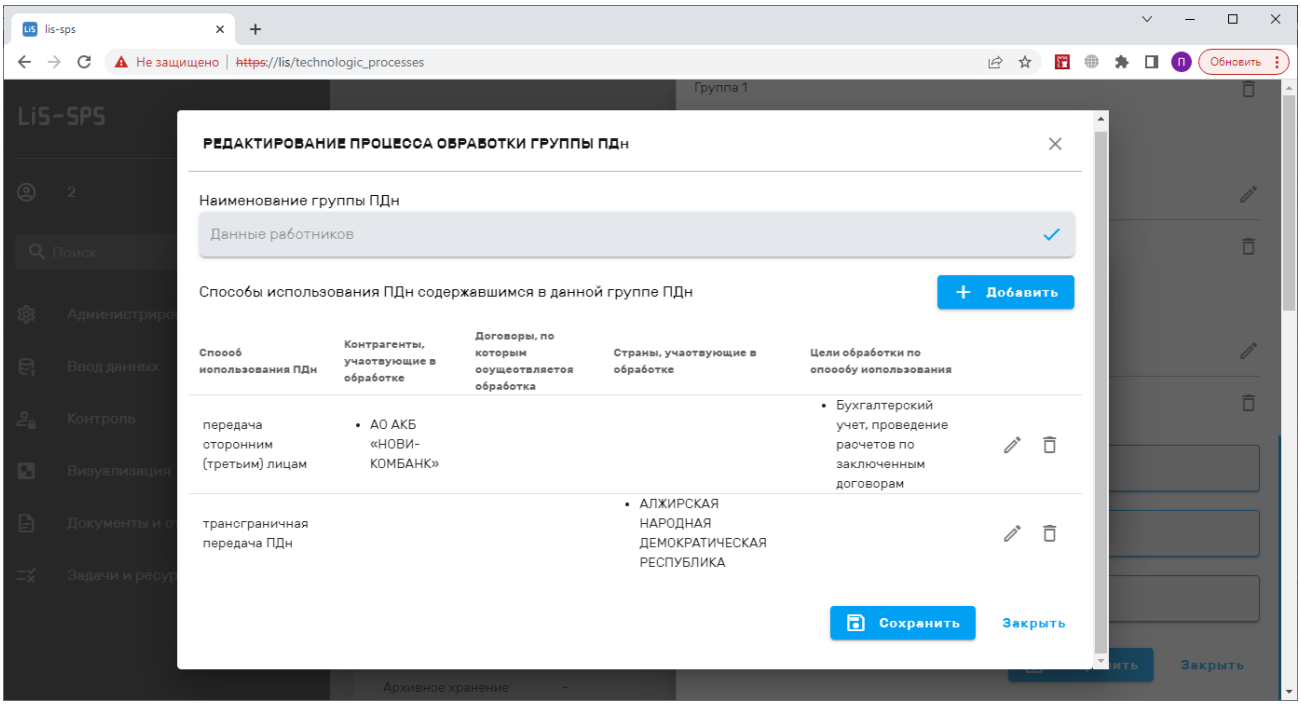

Рисунок 1 - Пример задания сведений о ПДн в интерфейсе «Технологические процессы»

1.3. учет возможности трансграничной передачи ПДн по каждому процессу с указанием стран, в которые осуществляется такая передача,

1.4. учет по каждому процессу источников получения ПДн (от субъектов ПДн лично, от третьих лиц),

1.5. учет объема, категорий (абоненты, посетители и т.п.) лиц, данные которых обрабатываются в каждом процессе, категорий ПДн (ФИО, номер телефона, адрес и т.п.) по каждой категории лиц обрабатываемых ПДн, способов обработки ПДн (использование, передача в третьи страны, поручение на обработку и т.п.) с привязкой к целям обработки ПДн,

[1] К функциям продукта «LIS-SPS»

1.6. автоматический контроль соответствия целей обработки ПДн, целям заранее заявленным,

1.7. обеспечение возможности согласования процесса ответственными лицами с отслеживанием версий процесса, простановкой электронной подписи.

2. Управление зданиями и помещениями, участвующими в обработке ПДн, включая:

2.1. задание для помещений тех, в которых производится обработка ПДн (как автоматизированная, так и неавтоматизированная),

2.2. учет помещений, в которых производится хранение съемных машинных носителей ПДн,

2.3. учет выполнения требований по защите помещений, в которых производится обработка ПДн, находятся машинные носители ПДн (наличие замков, решеток на окнах, надежных хранилищ для бумажных носителей ПДн при их неавтоматизированной обработке),

2.4. автоматический контроль необходимости обеспечения защиты помещений, в которых производится обработка ПДн посредством анализа внесенной информации о состоянии защиты помещений, наличия ПДн, характеристик расположения помещения (выход окон за пределы КЗ, возможность наличия посторонних лиц и т.п.).

3. Учет информационных активов, содержащих ПДн, включая:

3.1. задание для информационных активов информации о наличии ПДн (баз данных, файлов, бумажных документов, сервисов и т.п.), категорий лиц и состава обрабатываемых ПДн в информационных активах, характеристик режима обработки и разграничения доступа, других значимых характеристик,

3.2. автоматический расчет категорий ПДн содержащихся в активе,

3.3. обеспечение возможности ручного задания категории ПДн содержащихся в активе.

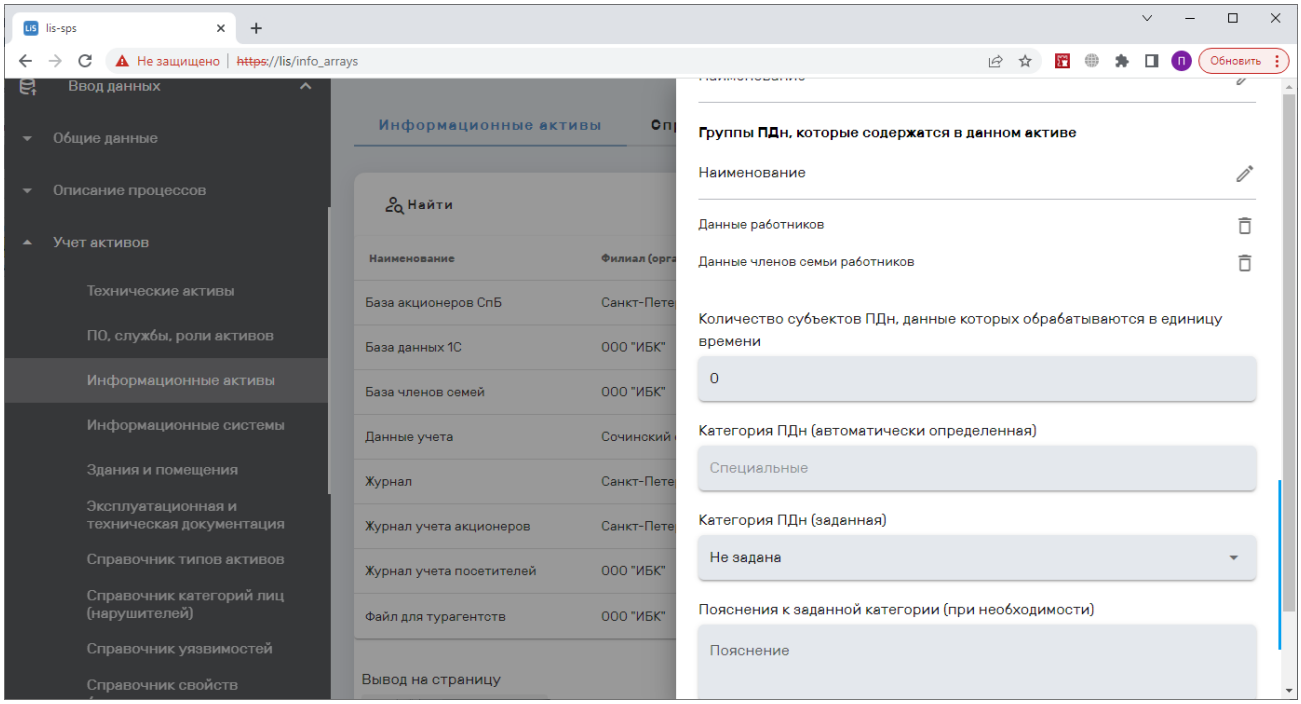

Рисунок 2 - Пример задания сведений о ПДн в интерфейсе «Информационные активы»

4. Контроль уничтожения ПДн при достижении целей обработки ПДн, включая:

4.1. ведение базы данных субъектов ПДн с заданием их ФИО, паспортных данных, принадлежности к тем или иным информационным активам,

4.2. учет произвольных характерных дат (дат, при наступлении которых начинается отсчет до конкретной даты уничтожения ПДн) по каждому субъекту ПДн позволяющих отслеживать сроки уничтожения ПДн,

4.3. автоматическое определение состава характерных дат, значимых для субъекта ПДн, посредством анализа процессов обработки ПДн, в которых участвуют ПДн данного субъекта ПДн,

4.4. задание сроков наступления характерных дат по каждому субъекту ПДн,

4.5. автоматический контроль своевременности уничтожения ПДн по каждому субъекту ПДн при окончании всех дат, которые заведены на данного субъекта ПДн.

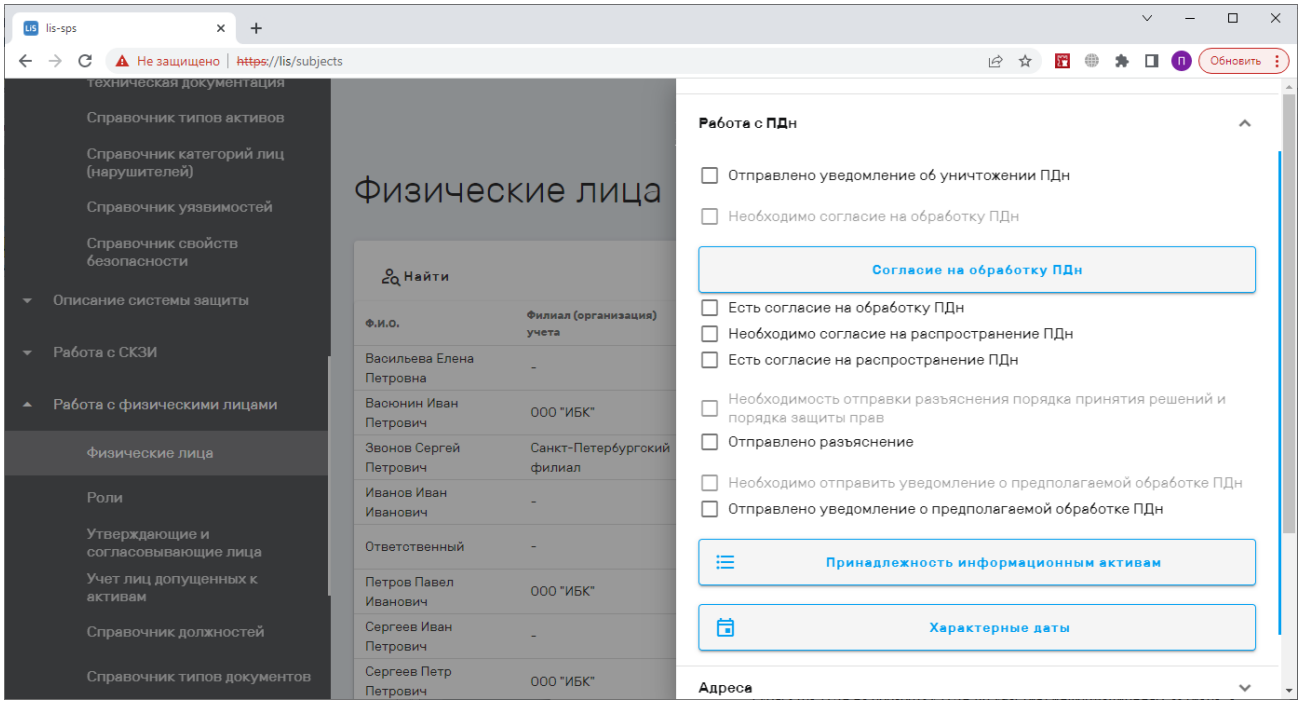

Рисунок 3 - Пример задания сведений о ПДн в интерфейсе «Физические лица»

5. Контроль наличия и генерация согласий на обработку ПДн, включая:

5.1. автоматическое определение необходимости получения согласий субъектов ПДн на обработку ПДн по участию информационных активов, в которых содержатся данные субъектов в процессах обработки ПДн требующих сбора согласий,

5.2. учет наличия согласий конкретных субъектов ПДн на обработку ПДн,

5.3. автоматический контроль необходимости получения согласий на обработку ПДн от конкретных субъектов ПДн,

5.4. генерация формы согласия на обработку ПДн с автоматическим включением в нее всех необходимых данных в зависимости от процессов обработки ПДн, в которых участвуют ПДн данного субъекта ПДн,

5.5. автоматический контроль наличия согласий на обработку ПДн от конкретных субъектов ПДн.

6. Категорирование ПДн, включая:

6.1. задание произвольных правил определения категории ПДн по категориям отдельных составов ПДн в целях автоматического определения категории ПДн обрабатываемых в информационных активах.

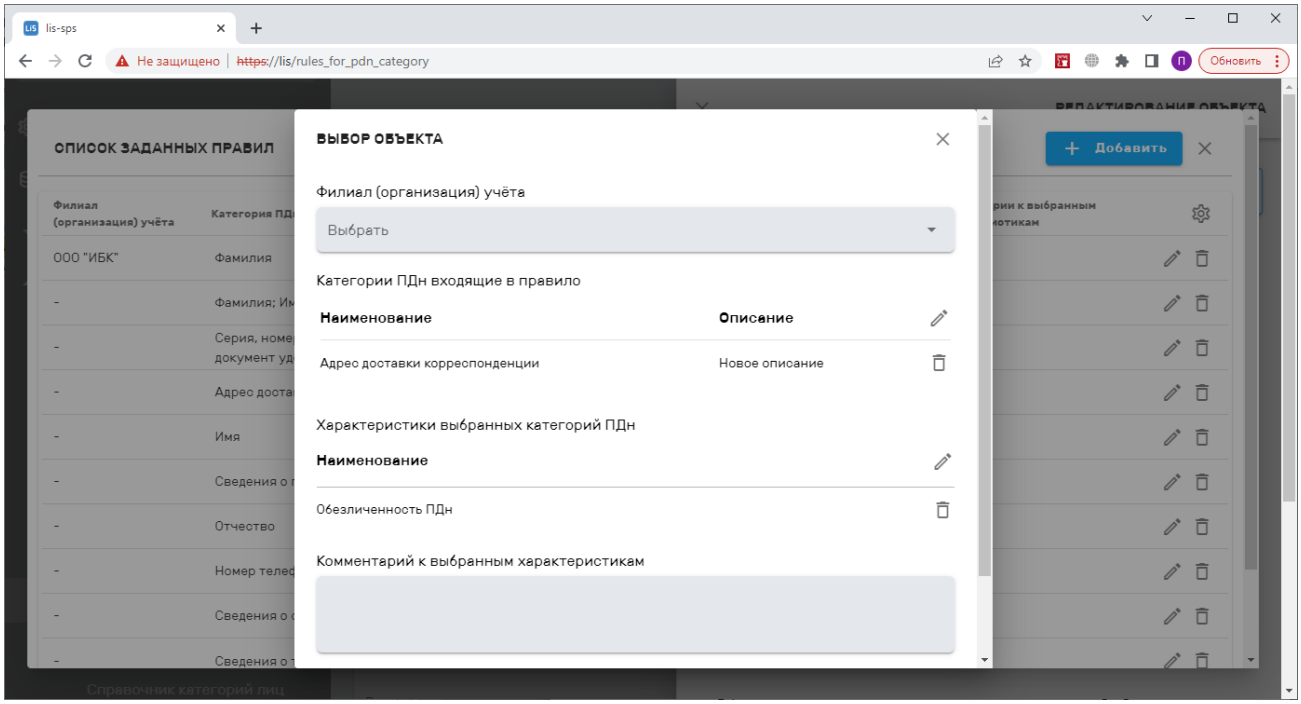

Рисунок 4 - Пример интерфейса «Правила определения категории ПДн»

7. Управление контрагентами, включая:

7.1. учет контрагентов, которым поручена обработка ПДн,

7.2. учет наличия поручений на обработку ПДн,

7.3. учет дат получения и истечения срока поручений на обработку по каждому договору контрагента,

7.4. автоматический контроль истечения срока поручения до окончания срока действия договора,

7.5. автоматический контроль наличия поручений на обработку ПДн,

7.6. возможность вложения файлов договоров (поручений) на обработку ПДн,

7.7. возможность учета средств защиты, категорий информации переданных в рамках договора (поручения).

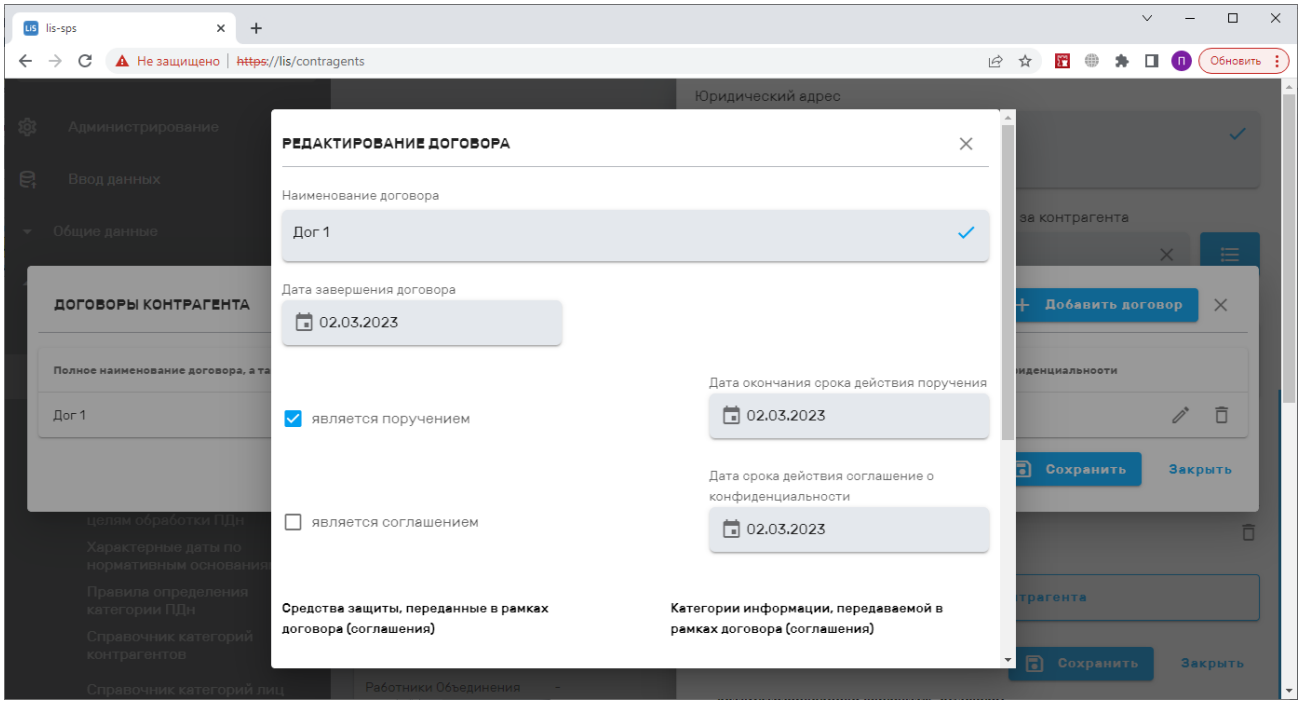

Рисунок 5 - Пример задания сведений о ПДн в интерфейсе «Контрагенты»

8. Учет и контроль разъяснений порядка принятия решений при исключительно автоматизированной обработке, включая:

8.1. учет юридических последствий, которые может повлечь за собой обработка ПДн в ИСПДн в целях генерации разъяснения порядка принятия решений при исключительно автоматизированной обработке,

8.2. учет порядка защиты субъектом ПДн своих прав и законных интересов и порядка принятия решения при исключительно автоматизированной обработке в целях генерации разъяснения порядка принятия решений при исключительно автоматизированной обработке,

8.3. автоматическое определение субъектов ПДн, которым надо разъяснить порядок принятия решений при исключительно автоматизированной обработке на основании принадлежности субъекта ПДн к активам, в которых осуществляется принятие таких решений,

8.4. учет отправленных разъяснений порядка принятия решений при исключительно автоматизированной обработке.

9. Учет и контроль Уведомлений о предполагаемой обработке ПДн, включая:

9.1. автоматическое определение состава субъектов ПДн, для которых надо генерировать Уведомление о предполагаемой обработке их ПДн,

9.2. учет отправки Уведомлений о предполагаемой обработке ПДн субъектам ПДн,

9.3. автоматический контроль уведомления субъекта ПДн до начала обработки его ПДн, посредством анализа наличия уже отправленного уведомления.

10. Учет ИСПДн, включая:

10.1. задание наименований ИСПДн их характеристик,

10.2. описание общих существенных для обработки ПДн характеристик ИСПДн (объем обрабатываемых ПДн, осуществляемые операции с ПДн).

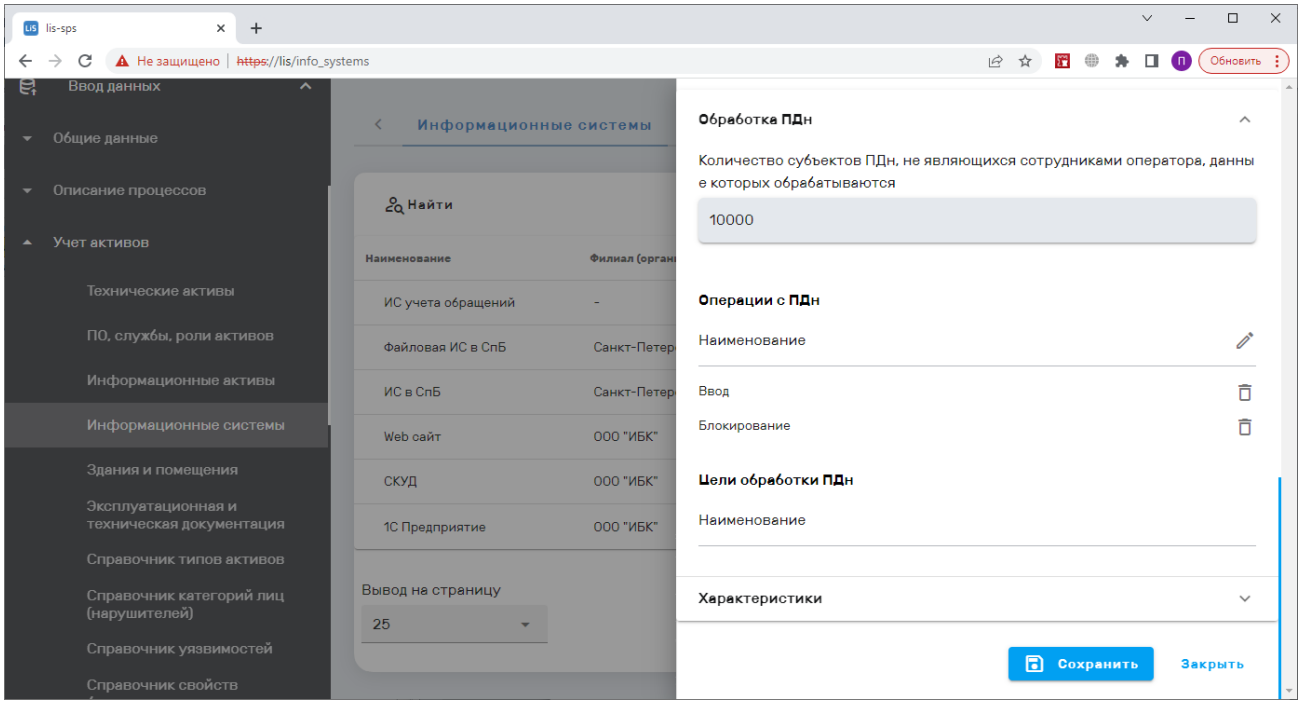

Рисунок 6 - Пример задания сведений о ПДн в интерфейсе «Информационные системы»

11. Управление уровнем защищенности ПДн, включая:

11.1. определение уровня защищенности ПДн посредством автоматического определений категорий ПДн, характеристик ИСПДн включаемых в акт,

11.2. фиксация данных указанных в текущем акте определения уровня защищенности ИСПДн,

11.3. автоматический контроль необходимости изменения уровня защищенности ИСПДн посредством анализа изменений в данных используемых для определения уровня и сравнении их с данными указанными в текущем уровне.

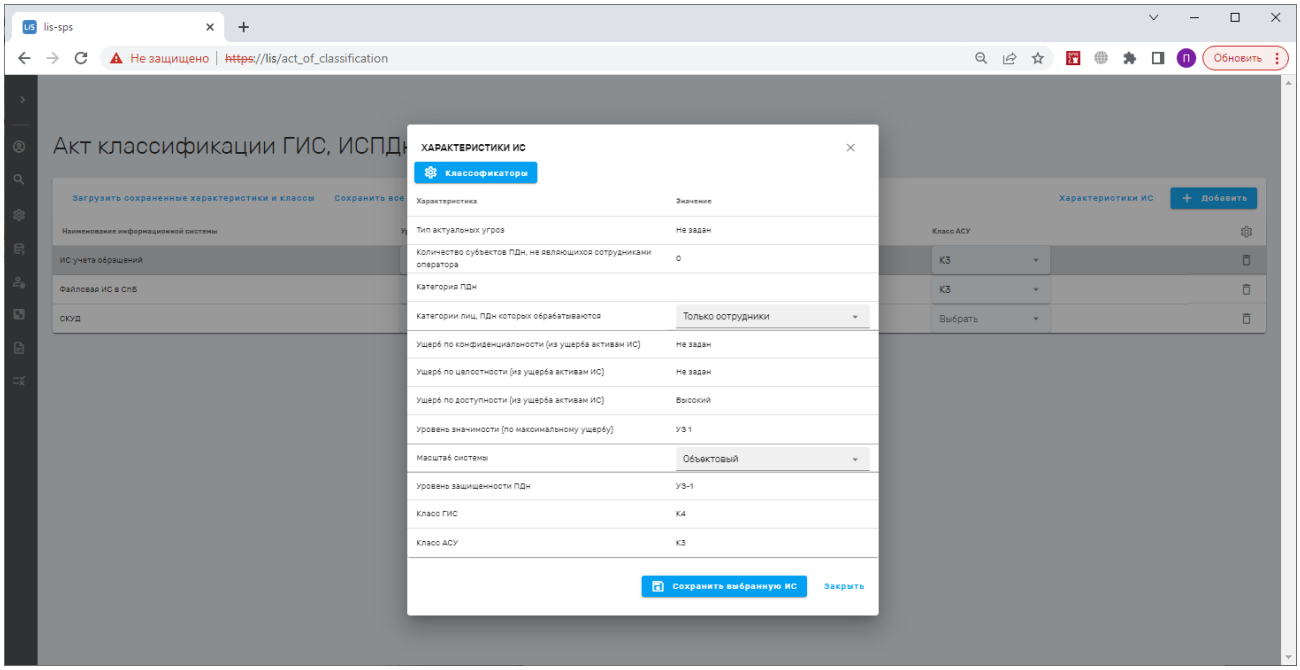

Рисунок 7 - Пример определения уровня защищенности ПДн

12. Управление контролем защищенности ПДн, включая:

12.1. учет проведенных контролей уровня защищенности ПДн и соблюдения условий использования средств защиты,

12.2. автоматическое формирование необходимых для проверки описаний функций защиты, средств защиты, процессов обработки ПДн,

12.3. автоматический контроль необходимости проведения контроля защищенности ПДн и соблюдения условий использования средств защиты с учетом даты проведения предыдущего контроля и требуемой частоты проведения контроля,

12.4. генерация формы акта на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты для конкретных активов с автоматическим указанием функций, которые должны быть проконтролированы,

12.5. генерация формы приказа на проведение контроля защищенности ПДн и соблюдения условий использования средств защиты для конкретных активов.

13. Управление Перечнем ПДн, включая:

13.1. автоматическая генерация перечня персональных данных, с включением в документ данных по обрабатываемым ПДн из указанных в процессах обработки;

13.2. автоматический контроль необходимости актуализации перечня персональных данных по наличию изменений в составе обрабатываемых ПДн в процессах.

2.2. Генерируемые документы

СПП ПДн в процессе своей работы, дополнительно, обеспечивает возможность автоматической генерации следующих документов:

1) Перечня ПДн
2) Приказа об определении мест хранения ПДн
3) Согласий на обработку ПДн
4) Акт контроля защищенности ПДн
5) Приказ на проведение контроля защищенности ПДн

3. Нормативные документы

Функции системы разработаны с учетом требований следующих нормативных документов:

- Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»
- Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства РФ от 15 сентября 2008 г N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»